UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/266,207	03/10/1999	PAUL ENGLAND	777.215US1	5470

22801 7590 04/25/2006

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
KLIMACH, PAULA W	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 04/25/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/266,207	ENGLAND ET AL.	
	Examiner	Art Unit	
	Paula W. Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 February 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *3-18* is/are allowed.

6)☒ Claim(s) *1,2 and 19-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2/1/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 02/01/06. The amendment filed on 02/01/06 have been entered and made of record. Therefore, presently pending claims are 1-21.

Response to Arguments

Applicant's arguments filed 02/01/06 have been fully considered but they are not persuasive because of following reasons.

Applicant argued that Arbaugh discloses setting a particular register (the software identity register) to a result of a computed cryptographic function if atomic execution of a boot block of the operating system does not fail. This is not found persuasive. The combination of Arbaugh and Anderson disclose the limitation of setting the result of a computed cryptographic function if atomic execution of a boot block of the operating system does not fail. In the combination of Arbaugh and Anderson, Arbaugh discloses a POST system, a system for verifying software, wherein the verification is performed using a cryptographic system. Further in the combination of Arbaugh and Anderson, Anderson discloses using the POST verification system to set the PREV_BOOT_FAIL flag to the result of the verification. Therefore in the combination Arbaugh would teach the POST system and Anderson discloses setting a memory value to a result of the POST.

Applicant argued that nowhere in Angelo, Arbaugh, or Anderson is there any discussion or mention of having a single software identity register that is set to a cryptographic hash of

Arbaugh under certain circumstances and is set as a determiner of Anderson under other circumstances. This is not found persuasive. The claims do not recite "a single software register that is set to a cryptographic hash."

Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2 are rejected under 35 U.S.C. 103(a) as being unpatentable over Angelo (5,944,82 1) in view of Arbaugh and further in view of Anderson (5,974,546).

In reference to claim 1, Angelo discloses a system that comprises a central processing unit (CPU: part 100 Fig. 1 in combination with column 6 lines 8-13) and an operating system (OS), the CPU having a software identity register (Fig. 2 in combination with column 9 lines 35-38), a method for booting the operating system. The secure location is memory and therefore performs the same function as the register of the software identity register. Furthermore Angelo discloses setting the software identity register to a result of the computed hash value (Fig. 3 and Fig. 4).

Although Angelo discloses saving the hash value (identity of the program) in memory, Angelo does not expressly disclose computing a cryptographic function of at least a portion of the operating system and setting the software identity register to a result of the computed cryptographic function.

Arbaugh discloses a system that verifies the kernel (operating system) by calculating the cryptographic and storing the hash of the operating system level (page 4 section 3.2. 1 paragraph

2 in combination with section 3.2.2 paragraph 4). The cryptographic hash is the identity of the operating system since it is used to verify the integrity of the system.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to calculate the cryptographic hash of the operating system as in Arbaugh in the system of Angelo. One of ordinary skill in the art would have been motivated to do this because calculating the cryptographic hah function is used to calculate the integrity of a function a system is then said to posses integrity, without integrity no system can be made secure (Arbaugh Introduction).

Although Arbaugh discloses a system that verifies the kernel by calculating the cryptographic and storing the hash of the operating system level (page 4 section 3.2. 1 paragraph 2 in combination with section 3.2.2 paragraph 4), the combination of Arbaugh and Angelo do not disclose setting the software identity register to a value indicating that the atomic execution of the boot block failed if the atomic execution of the boot block does not fail.

Anderson discloses a system wherein if the atomic execution of the boot block does not fail, and otherwise setting the software identity register to a value indicating that the atomic execution of the boot block failed (column 5 lines 34-41).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to set the software identity register of Angelo with a value indicating that the atomic execution of the boot block failed as in Anderson. One of ordinary skill in the art would have been motivated to do this because it would enable the system to determine the cause of a previously failed system boot and based on the analysis, selectively modify specific features and/or system parameters responsive to the cause of the failure during a previous system boot.

In reference to claim 2, Angelo discloses further a method comprising defining a secure storage space, access to which is based in part on the result set in the software identity register (column 9 lines 12-25). The integrity of the huh table is verified by the table hash value stored in the SMM memory.

Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hannah (6,735696 B1) and further in view of Stallings (Cryptography and Network Security).

In reference to claim 19, Hannah discloses a method and apparatus for booting an operating system (abstract). The system includes creating an OS certificate including the identity from the software identity register, information describing the operating system (column 3 lines 1-19). The checksum forming the identity of operating system.

Although Hannah discloses the operating system certificate, however Hannah did not disclose expressly the private key.

Stallings discloses verification using digital certificates (pages 186-187). The OS certificate would be signed using the CPU private key if the private key of the CPU is the same as the private key of the CPU.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize digital certificates for the verification process of Stalling instead of the system disclosed by Hannah. One of ordinary skill in the art would have been motivated to do this because any participant can verify that the certificate originated from the certificate authority and is not counterfeit.

Claims 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hannnah, and Stallings as applied to claims 19 above, and further in view of LeBourgeois (6,026,166).

LeBourgeois further suggests submitting the signed software identity register (the identity of the user) over a network to a third party to prove an identity of the operating system to the third party (Fig 3A and Fig. 3B).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to bind the identification of the device drive to the signature of the certificate as in LeBourgeois in the system of Angelo. One of ordinary skill in the art would have been motivated to do this because it is useful in ensuring that digital products are authorized for use on only one machine (column 3 lines 21-23).

Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Angelo, Arbaugh, and Anderson as applied to claims 3, 11, 19 are respectively above, and further in view of Sadowsky et al (6,230,285 B1).

In reference to claims 21, the method wherein creating an identity of the OS comprises forming the OS certificate with one or more items from a boot log containing identities of software components that are executing on the CPU. The boot log discussed by Sadowsky contains information such as the device driver and executables (column 4 lines 65 and 66). This information is shared with the certificate information suggested by Barr.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to append the identity to the boot log of Sadowsky in the system of Angelo. One

of ordinary skill in the art would have been motivated to do this because it will show the cause of boot failure (column 5 lines 12-15).

Allowable Subject Matter

Claims 3-18 are allowed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-38544. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Monday, April 17, 2006

HOSUK SONG
PRIMARY EXAMINER